

UNITED STATES DISTRICT COURT

FILED

JAN 30 2025

for the

Northern District of Oklahoma

Heldi D. Campbell, Clerk
U.S. DISTRICT COURTIn the Matter of the Search of
1049 North Gary Place, Apartment 15,
Tulsa, OK 74110Case No. 25-MJ-77-JFJFILED UNDER SEAL**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

18 U.S.C. § 1591(a)(1) and (b)(1)

Sex Trafficking of Children

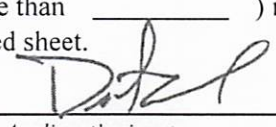
18 U.S.C. § 2422(b)

Coercion or Enticement


The application is based on these facts:

See Affidavit of HSI SA Dustin Carder, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signatureDustin Carder, HSI SA
Printed name and title

Subscribed and sworn to by phone.

Date: 1/30/25
Judge's signatureCity and state: Tulsa, OklahomaJodi F. Jayne, U.S. Magistrate Judge
Printed name and title

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for three separate search warrants for the locations and person specifically described in Attachment A of the respective affidavit and applications, including:

a. Search Warrant 1: the entire property located at 1049 North Gary Place, Apartment 15, Tulsa, OK 74110, Tulsa County, Northern District of Oklahoma, (“Subject Residence”);

b. Search Warrant 2: the vehicle described as a black 2019 Mitsubishi Outlander with Oklahoma License Plate KGZ-518 and VIN: JA4AZ3A31KZ044036, (“Subject Vehicle”); and

c. Search Warrant 3: the person of Timothy James Hall, Date of Birth: xx/xx/1995 (“HALL”),

as well as the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1591(a)(1) and (b)(1) (Sex Trafficking of Children), and 18 U.S.C. § 2422(b) (Coercion or Enticement), which items are more specifically described in Attachment B of this affidavit.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since December 2018. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child sex trafficking, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's ("FLETC") twelve-week Criminal Investigator Training Program ("CITP") and the sixteen-week Homeland Security Investigations Special Agent Training ("HSISAT") program, and everyday work relating to conducting these types of investigations. I have received training in the area of child sex trafficking, coercion or enticement of a minor, child exploitation, and child pornography. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, correlations between child pornography and hands-on offenses, psychological and behavioral characteristics of sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is

engaged in enforcing the criminal laws, including 18 U.S.C. §§ 1591, 2251, 2252, 2241, and 2422.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 1591(a)(1) and (b)(1) (Sex Trafficking of Children), and 18 U.S.C. § 2422(b) (Coercion or Enticement) will be located at 1049 North Gary Place, Apartment 15, Tulsa, OK 74110, Tulsa County, Northern District of Oklahoma (Search Warrant 1); within HALL's black 2019 Mitsubishi Outlander with Oklahoma License Plate KGZ-518 and VIN: JA4AZ3A31KZ044036 (Search Warrant 2); and on the person of HALL (Search Warrant 3), as further described in Attachment A of each respective application.

Jurisdiction

6. “[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.” 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

- a. 18 U.S.C. § 1591(a)(1) and (b)(1) (Sex Trafficking of Children),
- b. 18 U.S.C. § 2422(b) (Coercion or Enticement)

8. Venue is proper because the person and places to be searched are located within the Northern District of Oklahoma.

Definitions

9. The following definitions, inclusive of all definitions contained in 18 U.S.C. §§ 1591, 2246, and 2256, apply to this affidavit and the attachments incorporated herein:

- a. “Commercial sex act,” as defined in 18 U.S.C. § 1591(e)(3), is any sex act, on account of which anything of value is given to or received by any person.
- b. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in

sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;

d. “Internet Protocol address” or “IP address” refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet;

e. “Electronic Mail,” commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of

the most common methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

f. A “hash value” or “hash ID” is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file’s content. A hash value is a file’s “digital fingerprint” or “digital DNA.” Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file’s hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

g. “Cloud storage service” refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

h. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

- i. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;
- j. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and
- k. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Background on Digital Media Storage Devices

10. The ability of a computer (including a smartphone) to store images in digital form makes the computer itself an ideal repository for child pornography or evidence of child exploitation and trafficking. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Given the storage capabilities, modern computers can retain many years’ worth of a user’s data, stored indefinitely. Even deleted data can

often be forensically recovered. Other digital media storage devices (e.g., compact disks, digital video disks, thumb drives, etc.) can also store tremendous amounts of digital information, including digital video and picture files.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Further, even if deleted, forensic examination can sometimes recover files and data including deleted picture files. I know that computers such as laptops, iPhones, and other smartphones can be forensically examined, and forensic analysts can learn much detail about the user's habits and online activities, including websites visited, files downloaded, Google searches performed, locations where the device was used, dominion and control information, etc.

12. Computers and other digital file storage devices can store the equivalent of thousands of pages of digital information. Especially when the user wants to conceal

criminal evidence, he or she often stores it in random order with deceptive file names. This requires the searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks depending on the volume of the data stored, and it would be generally impossible to accomplish this kind of data search on site. Furthermore, I know that smartphones (a type of “computer,” as broadly defined in 18 U.S.C. § 1030(e)(1)) like an iPhone can typically “sync” with a traditional desktop or laptop computer. The purpose of syncing a smartphone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smartphone is lost or damaged. Also, smartphone users may move files off the smartphone and onto a computer to free up storage space on the smartphone. Similarly, computer (e.g., desktop computers, smartphones, etc.) users may move files off of one computer onto another computer or digital file storage devices such as a thumb drive, a DVD, an external hard drive to free up space on the computer. For this reason, I am seeking authorization to seize all computers and digital file storage devices at the Subject Residence, within the Subject Vehicle, and on the person of HALL—not any particular computer.

Probable Cause

13. In August 2024, the HSI Tulsa-led Tornado Alley Child Exploitation and Trafficking Taskforce (“TACETT”) assisted the Collinsville, Oklahoma Police Department (“CPD”) with an investigation involving a 12-year-old minor victim (“MV1”), and suspects J.R. and J.M. J.R. is an enrolled member of the Cherokee

Nation tribe and is the mother of MV1. J.M. is the boyfriend of J.R. Both subjects are currently charged in the Northern District of Oklahoma in relation to the sexual abuse of MV1.

14. During the above investigation into J.R. and J.M., it was discovered that MV1 previously disclosed to J.R. about sexual abuse committed by Timothy James HALL, one of J.R.'s ex-boyfriends. When this disclosure was made in 2023, J.R. notified CPD of the incident. CPD reported that on January 26, 2023, Officer Grant Thornton responded to a residence in Collinsville, Oklahoma, within the Northern District of Oklahoma, regarding a juvenile that did not want to return to her mother's boyfriend's house because he wanted to do sexual activities with the juvenile. At the time of the report, MV1 was ten years old. J.R. told the officer that MV1 disclosed that J.R.'s boyfriend, HALL, asked MV1 to engage in sexual activities with him. J.R. told Officer Thornton that this happened at **1049 North Gary Place, Tulsa, Oklahoma.**

15. J.R. completed a witness statement and stated that the first incident occurred in December of 2022. J.R. wrote that HALL stayed up late and she was asleep. J.R. wrote that HALL talked to MV1 about having sex with his stepchildren, and that HALL's stepfather did it with his sisters to train them for life. J.R. also wrote about other incidents where HALL would take MV1 with him to deliver Amazon packages when J.R. was ill. While making deliveries, HALL discussed doing sexual things to other little girls and paying to have sexual contact with them. HALL also tried to

force MV1 to perform oral sex on him. CPD completed an information report and forwarded it to the Tulsa Police Department (“TPD”) since the incidents occurred in Tulsa.

16. TPD Detective Paula Maker received the referral report from CPD. In Detective Maker’s report, she documented that she attempted to contact J.R. regarding the allegations; however, J.R.’s phone number was out of service. On March 22, 2023, Detective Maker mailed a letter to J.R. using the address listed on the original police report. Detective Maker never received a response to the letter.

17. On November 12, 2024, I was contacted by Oklahoma Department of Human Services (OKDHS) Case Worker Debra Hanmer. Hanmer informed me that MV1 had made a recent disclosure regarding HALL. MV1 disclosed that HALL had sexually abused her when she was 9 or 10 years old, and that he discussed buying other girls. MV1 is currently in OKDHS custody and is placed with a relative.

18. On November 20, 2024, MV1 was forensically interviewed at the Child Abuse Network in Tulsa. The interview was audio and video recorded. The following paragraphs summarize statements made by MV1:

19. MV1 stated that she was here “because of Tim.” MV1 later stated his last name was HALL. HALL is MV1’s mother’s ex-boyfriend. MV1 stated that HALL had sexually abused her. MV1 described that one night, HALL came up to her in the kitchen while she was cooking and grabbed her from behind. HALL told her that he wanted to have sex with her. This occurred at HALL’s house in Tulsa when she was

9 or 10. MV1 was able to break free of his grasp and ran to a neighbor's apartment. MV1 asked the neighbor if she could stay there. MV1 ended up staying there for two days. MV1 did not tell her mom, J.R., what had happened with HALL because he threatened to hurt MV1, J.R., and MV1's siblings if she did say anything.

20. MV1 described another incident where she accompanied HALL as he was delivering Amazon packages. HALL attempted to molest her by placing his hand on her leg and moving it closer to her "private part." MV1 jumped out of the vehicle and a concerned citizen stopped to help. MV1 was not able to adequately explain what was happening with HALL to the concerned citizen. The concerned citizen talked to HALL, who explained away MV1's behavior by stating she was confused. HALL has also tried touching MV1's breasts and vagina over the clothes.

21. MV1 stated that HALL forced her to do things to him by starving her. HALL made her show him her breasts and vagina. HALL starved her by not allowing her to have food. HALL told MV1 that she would not eat unless she did stuff for him. The longest period she went without eating was three days.

22. MV1 described an incident where HALL handcuffed her to a bed, sat on her legs, and then forced her to show him her body. HALL's clothes were on during this time. HALL heard J.R. nearby in the house and stopped.

23. There was another incident described by MV1 where HALL forced her to perform oral sex on him. MV1 stated that it happened at HALL's house in the kitchen. Everyone else was asleep and J.R. was taking a shower. MV1 stated that

while he was forcing her to do this, she felt like she could not breathe sometimes. HALL stopped when he told her he was about to ejaculate and then went into the bathroom.

24. HALL commented to MV1 about how “hot” MV1’s minor cousin was also. MV1 was going to let her cousin know about HALL, but HALL told her he would kill her entire family if she did.

25. MV1 further described an incident where HALL told MV1 that he bought a 13-year-old girl off the internet, specifically TikTok¹. HALL told the 13-year-old girl that he was younger than he really was and sent fake pictures of himself. HALL asked the girl if he could talk to her father, and he did so. HALL told the girl’s father that he would pay \$100 per hour to have his way with the girl. HALL received photos of the girl in bikinis and showed them to MV1. MV1 stated that the girl was pretty, had long hair, and was wearing a two-piece bathing suit. One was blue and the other pink. The pictures of the girl were sent to HALL via text message. MV1 was unable to recall what kind of phone HALL had, except that it was an Android.

26. MV1 finally told J.R. what was happening when they were visiting at her aunt’s house in Collinsville. J.R. then called the cops to report it.

27. MV1 stated that HALL’s house was near an elementary school that she attended in the 3rd, 4th, and 5th grades. MV1 described the house as blue/gray with

¹ TikTok is a social media company owned by its Chinese parent company, ByteDance. TikTok allows users to create, watch, and share short videos shot on mobile devices or webcams. Users can also send each other messages.

houses around. J.R. reported to CPD that HALL's address was 1049 North Gary Place, Tulsa, OK 74110. Upon viewing this address in Google Maps², I observed these to be single-story apartments that are side by side. They are bluish gray in color. There are houses that surround the apartments. J.R. also provided HALL's date of birth as xx/xx/1995, or 1996. I queried Accurint³ for HALL with date of birth of xx/xx/1995, and located Timothy James HALL at **1049 North Gary Place, Apartment 15, Tulsa, OK 74110, the Subject Residence**. Accurint did not locate a Timothy HALL with the other date of birth.

28. On November 21, 2024, at approximately 0742 hours, I conducted physical surveillance at the Subject Residence. I observed a **black 2019 Mitsubishi Outlander with Oklahoma license plate KGZ-518, the Subject Vehicle**, parked in front of Apartment 15. A registration check revealed the vehicle is registered to HALL at the same address. According to the registration information, the VIN is JA4AZ3A31KZ044036.

29. I also noticed that on the mailbox next to the door of the apartment, no numbers were displayed on it. However, based on the numbers displayed on the

² Google Maps is a web service that provides detailed information about geographical regions and sites worldwide. In addition to conventional road maps, Google Maps offers aerial and satellite views of many locations. In some cities, Google Maps offers street views comprising photographs taken from vehicles.

³ LexisNexis' Accurint is online investigative software, similar to CLEAR, that provides law enforcement with a direct connection to public records to help verify identities, assets, and connections.

mailboxes of the other apartments next to it in sequential numerical order, I determined that HALL's vehicle was parked in front of Apartment 15.

30. I did not observe the numbers "1049" anywhere on the apartment building. The apartment building directly south of it displays "1041." In reviewing the address and location of the property in Google Maps, observing HALL's vehicle parked in front of Apartment 15, it is apparent that this particular building is "1049." There is a narrow alleyway between the two buildings; however, there is not a back door to the apartments. The front door and only entrance to the apartments in 1049 face north towards East Latimer Street. There are a total of six apartments in the 1049 single-story apartment building. Apartment 15 is the third apartment east of North Gary Place on the south side of East Latimer Street.

31. On January 3, 2025, I electronically served Amazon, HALL's employer, with an administrative Department of Homeland Security summons requesting information regarding HALL's work schedule as an Amazon Fulfillment employee.

32. On January 16, 2025, Amazon's legal representative responded to the summons and provided the requested information. The time frame of HALL's schedule provided by Amazon was January 1, 2024, through January 15, 2025. In reviewing the most recent data, HALL seems to mostly work between 6:30 PM to 5:30 or 6:00 AM.

33. On January 23, 2025, beginning at approximately 1715 hours, I conducted physical surveillance near the Subject Residence. I was in a stationary position at the

northwest corner of East Latimer Street and North Gary Place. At the beginning of surveillance, I observed the Subject Vehicle in front of Apartment 15.

34. At approximately 1800 hours, I observed a white male with facial hair wearing a black beanie, black T-shirt with a skeleton design, and khaki pants exit Apartment 15 walking a small dog. The subject then took the small dog inside and came back out with a larger dog. After putting that dog back in the apartment, the subject appeared to lock the door of the apartment and then entered the Subject Vehicle at 1813 hours. I then terminated surveillance. After comparing the surveillance photographs taken with HALL's Oklahoma driver's license photo, I positively identified the subject as HALL.

35. Based on the information described in this affidavit, I believe that evidence of the offenses listed herein will be located in the Subject Residence, the Subject Vehicle, and/or the person of HALL. Additionally, virtually every individual in today's society has at least a cellular phone or smartphone on their person or within their close reach at nearly all times of the day. These devices may also be found in their residence or vehicle where the individuals have immediate access and control. These devices often contain a vast amount of data about an individual's life, activities, and hobbies, illicit or not. It is probable to conclude that any evidence of the offenses cited herein would be located on HALL's devices. Lastly, MV1 has been forensically interviewed twice regarding the abuse she has endured. MV1's statements regarding J.R. and J.M. (*i.e.*, the case that has already been filed in the

Northern District of Oklahoma) have been corroborated by digital evidence and suspect admissions.

Characteristics Common to Individuals who Exhibit a Sexual Interest in Children

36. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;
- c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or

some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child

pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"⁴ it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and

⁴ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if HALL uses a portable device (such as a mobile phone) to access the internet, it is more likely than not that evidence of this access will be found in his home, the Subject Residence, and/or the Subject Vehicle, and/or the person of HALL, as set forth in Attachment A.

Common Practices of Persons Who Unlawfully Engage in Sex Trafficking

37. Based on my previous investigative experience related to sex trafficking investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who engage in sex trafficking:

- a. Sex trafficking can occur when parents or guardians act as a “pimp” to sell their children to others for sex. Many times, those situations arise when parents or guardians have a history in the sex trade and/or have drug or alcohol dependencies and exploit their children to satisfy their addictions.
- b. Sex traffickers almost always rely upon cellular telephones and computers to facilitate their business. Persons engaging in sex trafficking frequently communicate through text messaging, social media, email, and voice

communications via cellular phones. Additionally, sex traffickers use the same methods of communication to recruit and control victims, advertise, connect between supply and demand, dispatch sex workers to meet with potential buyers, discuss prices and meeting arrangements, communicate threats or promises to victims and buyers, and arrange for the acquisition, transportation, and laundering of proceeds generated from these illegal activities. They frequently maintain text messages, social media messages, and voice communications for long periods of time. In many cases, a sex trafficking victim will have a phone with her for a commercial sex transaction with an open and live call with the pimp, who listens to and monitors the encounter. In many instances, sex workers will use internet- and social media-based telephone numbers.

c. Traffickers and sex workers/victims frequently take and store photographs and video recordings on their cellular devices and/or computer and transmit those photos and videos via social media applications and the internet. These photographs often include photographs of the sex workers/victims, both sexually explicit and non-explicit, that can be posted as advertisements for unlawful commercial sexual activity. Buyers and sex workers frequently exchange photos for identification purposes, and supply-side participants frequently document their proceeds from unlawful commercial sex activities in what are referred to as “trophy photos.” These photos/videos also often include other sex workers, pimps, buyers and/or their associates.

d. Those that conspire or conduct transactions relating to human trafficking and/or unlawful commercial sex often identify themselves by monikers, street names, and/or nicknames to hinder law enforcement's efforts in identifying those involved with the commercial sex.

e. Sex workers and traffickers—both pimps and buyers—will often use coded words and phrases and vague conversations to discuss their plans and prevent anyone from overhearing their conversations and from recognizing that the conversations concern a commercial sex act.

f. Sex trafficking victims and sex workers are frequently advertised on a variety of social media platforms. These websites, applications, and platforms are often accessed by smartphones, cell phones, computers, and other similar devices. Individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

Background on Computers and the Internet

38. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers, smartphones⁵ and digital technology are the primary way in which individuals who exhibit a sexual interest in children and are interested in sex trafficking interact with each other.
- b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;
- c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Media and text files can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

⁵ Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for these illicit activities. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to search for children and/or methods to engage in sexual activities with children. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where

online storage is used, however, evidence of these activities can be found on the user's computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Systems

39. As described above and in Attachment B, this application seeks permission to search for records that might be found in the Subject Residence, and/or in the Subject Vehicle, and/or on the person of HALL in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrants applied for would authorize the seizure of electronic storage media or,

potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. I submit that if a computer or storage medium is found in the Subject Residence, and/or in the Subject Vehicle, and/or on the person of HALL, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file;
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information;

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

41. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Residence, and/or the Subject Vehicle, and/or the person of HALL because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified;

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity

can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to

destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

f. I know that when an individual uses a computer to obtain or access child pornography, or engage in sex trafficking or the coercion and enticement of a

minor, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of

computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to

conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

43. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called “wireless routers,” which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be “secured” (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or “unsecured” (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for

example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

44. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

Conclusion

45. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. § 1591(a)(1) and (b)(1) (Sex Trafficking of Children), and 18 U.S.C. § 2422(b) (Coercion or Enticement) have been violated, and that the contraband, property, evidence, fruits and instrumentalities of this offense, more fully described in Attachment B, are located at the sites described in Attachment A. I

respectfully request that this Court issue search warrants for the locations described in Attachment A, authorizing the search and seizure of the items described in Attachment B.

46. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,



Dustin L. Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on January 30th, 2025.



JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is a residence located at 1049 North Gary Place, Apartment 15, Tulsa, OK 74110, Tulsa County, Northern District of Oklahoma, (the Subject Residence), further described as a single-story apartment complex located at the southeast corner of North Gary Place and East Latimer Street in Tulsa, Oklahoma. The residence to be searched is Apartment 15, which is the third apartment east of North Gary Place on the south side of East Latimer Street. The apartment building is bluish gray in color. The residence to be searched has a white iron storm door.

The premises to be searched is located within the Northern District of Oklahoma, described above, and pictured below:





ATTACHMENT B

Particular Things to be Seized

All items that constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1591(a)(1) and (b)(1) (Sex Trafficking of Children), and 18 U.S.C. § 2422(b) (Coercion or Enticement) involving Timothy James HALL, including:

- a. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct, images/videos/gifs consistent with the advertisement or solicitation of an individual for commercial sex acts, to include the trafficking or buying of individuals, in any form wherever it may be stored or found including, but not limited to:
 - i. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other

computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, and/or the advertisement or solicitation of an individual for commercial sex acts;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to

the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts; and

iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts.

b. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256

or relating to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts;

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts;

iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts;

- iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors or a sexual interest in children, and/or the advertisement or solicitation of an individual for commercial sex acts;
 - v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
 - vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
 - vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
 - viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;
- c. Credit card information including, but not limited to, bills and payment records, and including, but not limited to, records of internet access;

d. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

e. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

f. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

g. Any data or materials establishing ownership, use or control of any computer equipment seized from the Subject Residence and/or the Subject Vehicle.

h. Any and all information, correspondence (including emails and text messages), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts, and/or the advertisement or solicitation of an individual for commercial sex acts.

i. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing);

any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

j. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

k. The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.